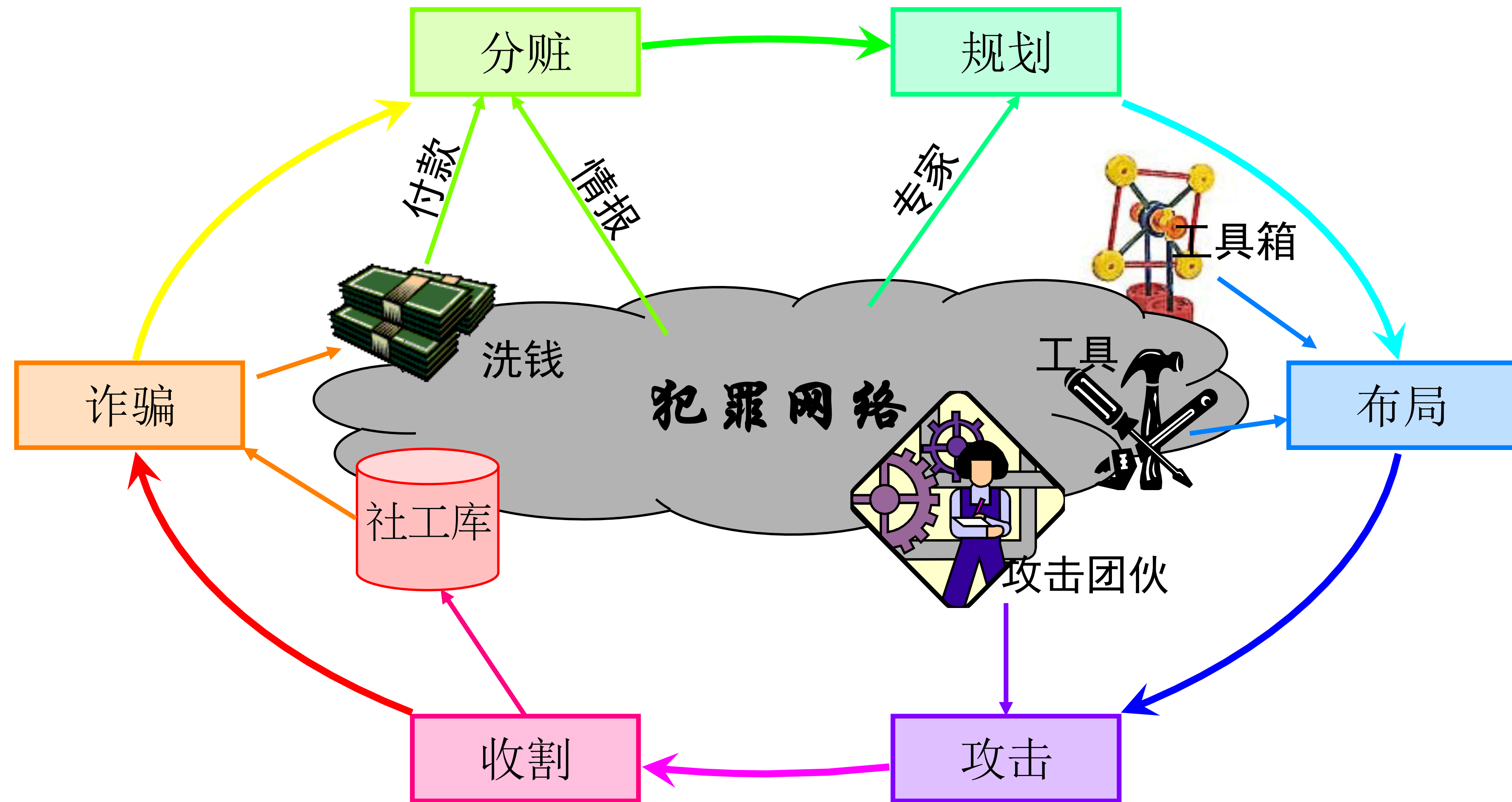


线上应用业务安全

 岂安科技

岂安，罗启武

每个人都有可能是坏的



75%

网络攻击的目标是网页应用

Source: Gartner

76%

网站具有漏洞

Source: Symantec

20%

网站漏洞是致命的

Source: Symantec

59%

网络流量来恶意爬虫

Source: distil networks

90%

攻击流量为自动化攻击

Source: Research and Markets

98%

攻击目标为易于攻击的目标

Source: Verizon

目录

应用载体

应用安全

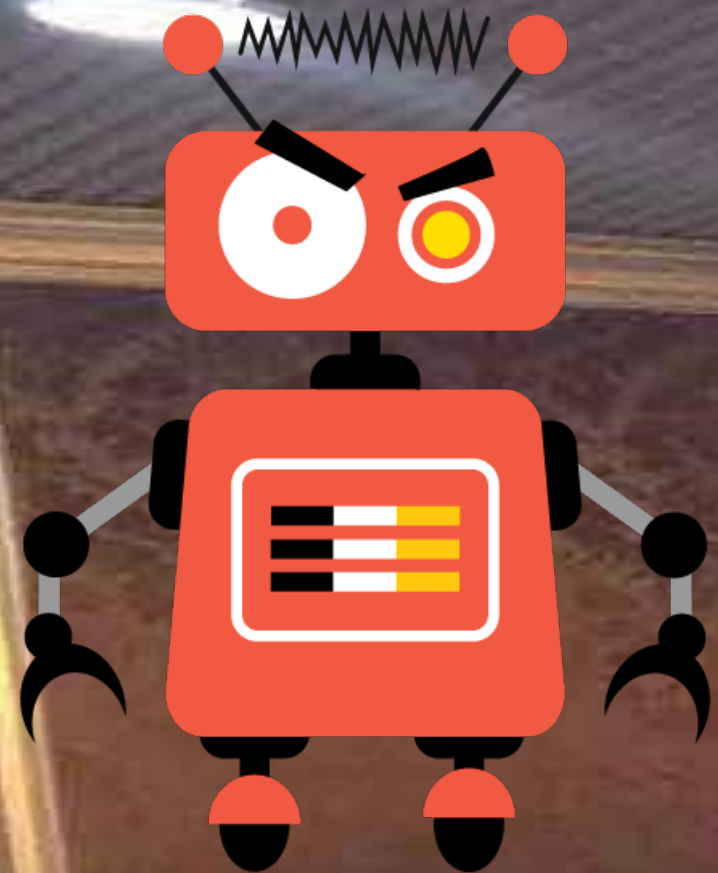
线上业务

一些思路



#移动载体

- OS组件 (Webview内/外部)
- 本地存储 (敏感信息/External/Internal/LocalDB/Images)
- 通讯安全(加密/验签/https/认证授权)
- 核心功能建议NDK, 代码保护, 加密/签名
- 其他/模拟器/越狱/终端环境等等



#应用安全

- 黑客漏洞攻击，应用/服务器
- 程序常规的安全漏洞（防火墙等）
- DDOS/CC
- 认证
- 隐私泄漏（用户敏感信息等）

当前位置: [WooYun](#) >> [漏洞信息](#)

漏洞概要

缺陷编号: **WooYun-2014-88532**

漏洞标题: 大量12306用户数据在互联网疯传包括用户帐号、明文密码、身份证邮箱等(泄漏途径目前未知)

相关厂商: [中国铁道科学研究院](#)漏洞作者: [追寻](#)

提交时间: 2014-12-27 10:59

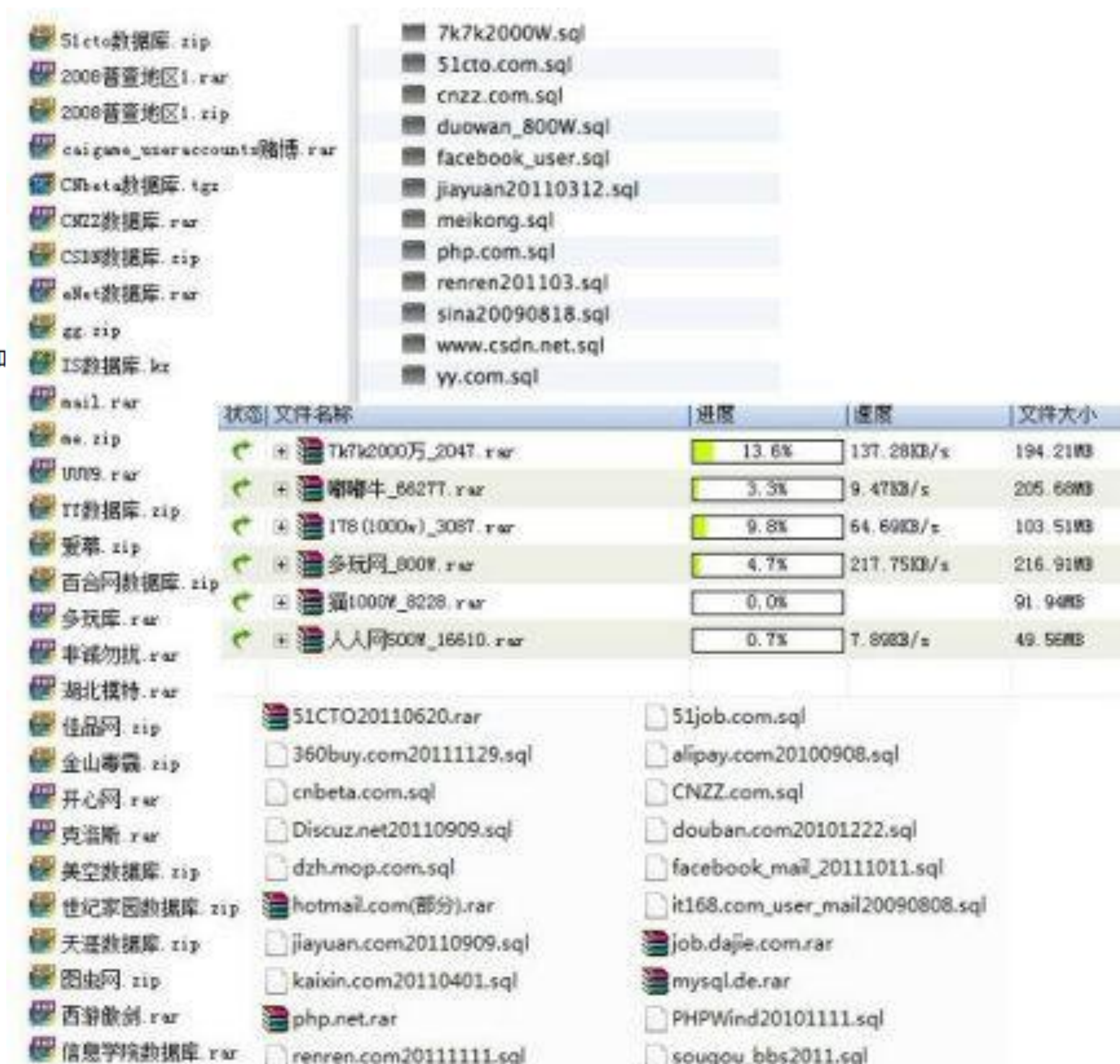
公开时间: 2015-02-08 11:00

漏洞类型: 用户资料大量泄漏

危害等级: 高

自评Rank: 10

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>Tags标签: [用户敏感信息泄漏](#) [用户敏感数据泄漏](#) [住址身份证姓名等敏感信息](#) [用户敏感信息泄露](#)

状态	文件名称	进度	速度	文件大小
+	Tk7k2000万_2047.rar	13.6%	137.28KB/s	194.21MB
+	嘟嘟牛_6627T.rar	3.3%	9.47KB/s	205.68MB
+	178(1000w)_3087.rar	9.8%	64.69KB/s	103.51MB
+	多玩网_800W.rar	4.7%	217.75KB/s	216.91MB
+	蜀1000W_8228.rar	0.0%		91.94MB
+	人人网500W_16610.rar	0.7%	7.89KB/s	49.56MB

51cto数据库.zip

2008普查地区1.rar

2008普查地区1.zip

caigame_useraccounts.rar

CNbeta数据库.tgz

CN22数据库.rar

CS13数据库.zip

eNet数据库.rar

gg.zip

IS数据库.kx

mail.rar

me.zip

U009.rar

IT数据库.zip

爱华.zip

百合网数据库.zip

多玩库.rar

非诚勿扰.rar

湖北模特.rar

佳品网.zip

金山毒霸.zip

开心网.rar

克洛斯.rar

美空数据库.zip

世纪家园数据库.zip

天涯数据库.zip

图虫网.zip

西游微剑.rar

信息学院数据库.rar

7k7k2000W.sql

51cto.com.sql

cnzz.com.sql

duowan_800W.sql

facebook_user.sql

jiayuan20110312.sql

meikong.sql

php.com.sql

renren201103.sql

sina20090818.sql

www.csdn.net.sql

yy.com.sql

51CTO20110620.rar

360buy.com20111129.sql

cnbeta.com.sql

Discuz.net20110909.sql

dzh.mop.com.sql

hotmail.com(部分).rar

jiayuan.com20110909.sql

kaixin.com20110401.sql

php.net.rar

renren.com20111111.sql

51job.com.sql

alipay.com20100908.sql

CNZZ.com.sql

douban.com20101222.sql

facebook_mail_20111011.sql

it168.com_user_mail20090808.sql

job.dajie.com.rar

mysql.de.rar

PHPWind20101111.sql

sougou_bbs2011.sql

#线上业务



产品宣传

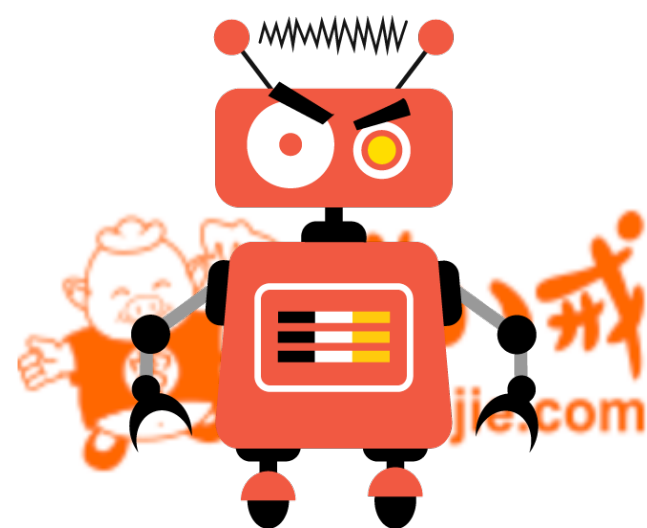
用户注册

用户登录

订单生成

支付

#机器人 bots



找服务 ▾ 年货包装设计特价，企业送礼倍有面儿

首页 > 工具软件

1,000元 电商网站接口爬虫接口，一共30多个，1000RMB/个

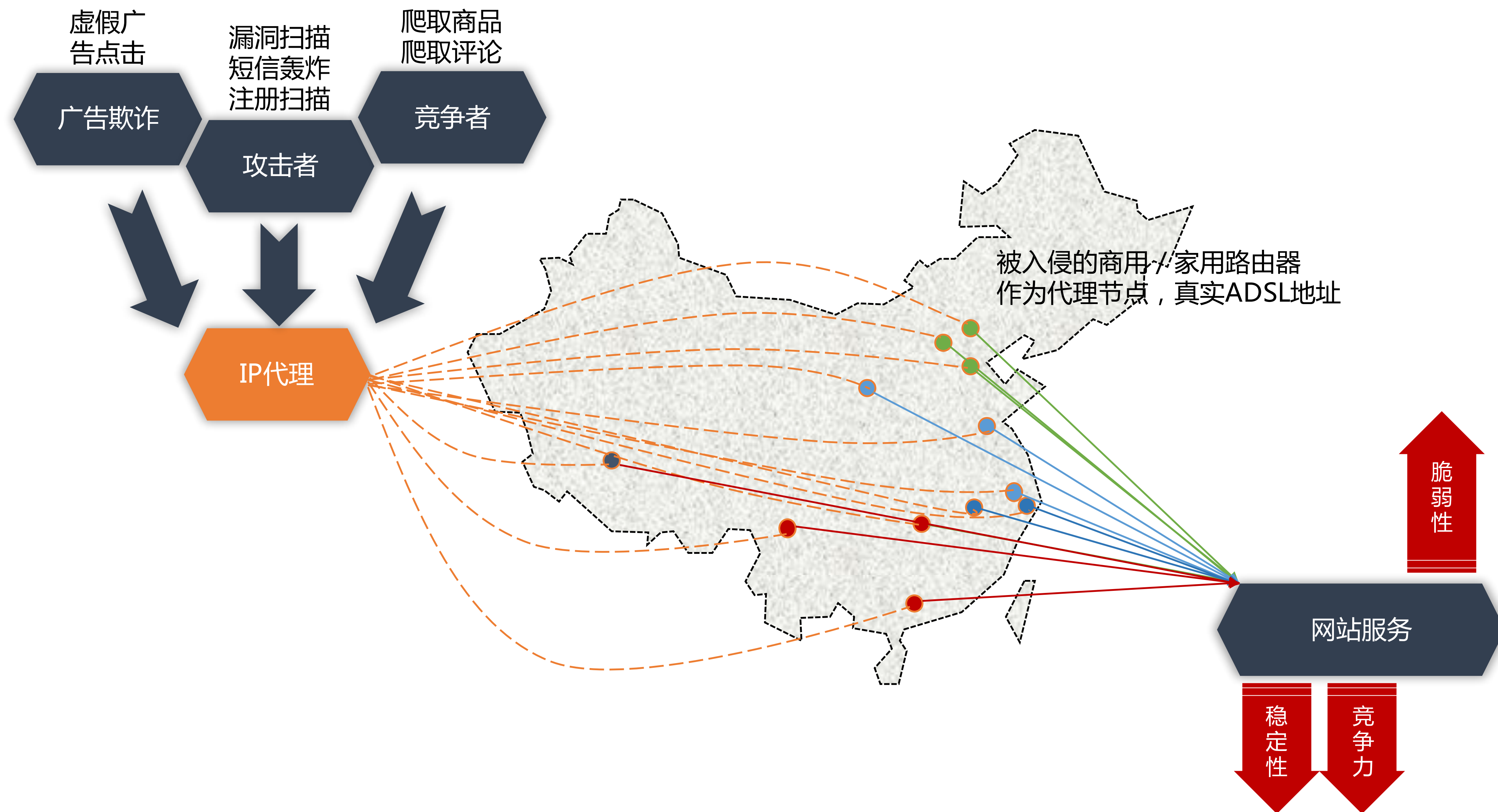
已有1个服务商中标，共有23个服务商投标，平均报价¥1000

需求描述：

需求：输入一个电商网站的任意商品网址，则返回该商品信息，比如标题、描述、价格等；可使用对方网站API(如果有的话)，也可使用爬虫方式；一共有30多个电商网站需要支持，1个1000RMB，1个起接！开发语言最好是python优先，使用PHP、JAVA亦可。

发布类似需求，获得免费报价

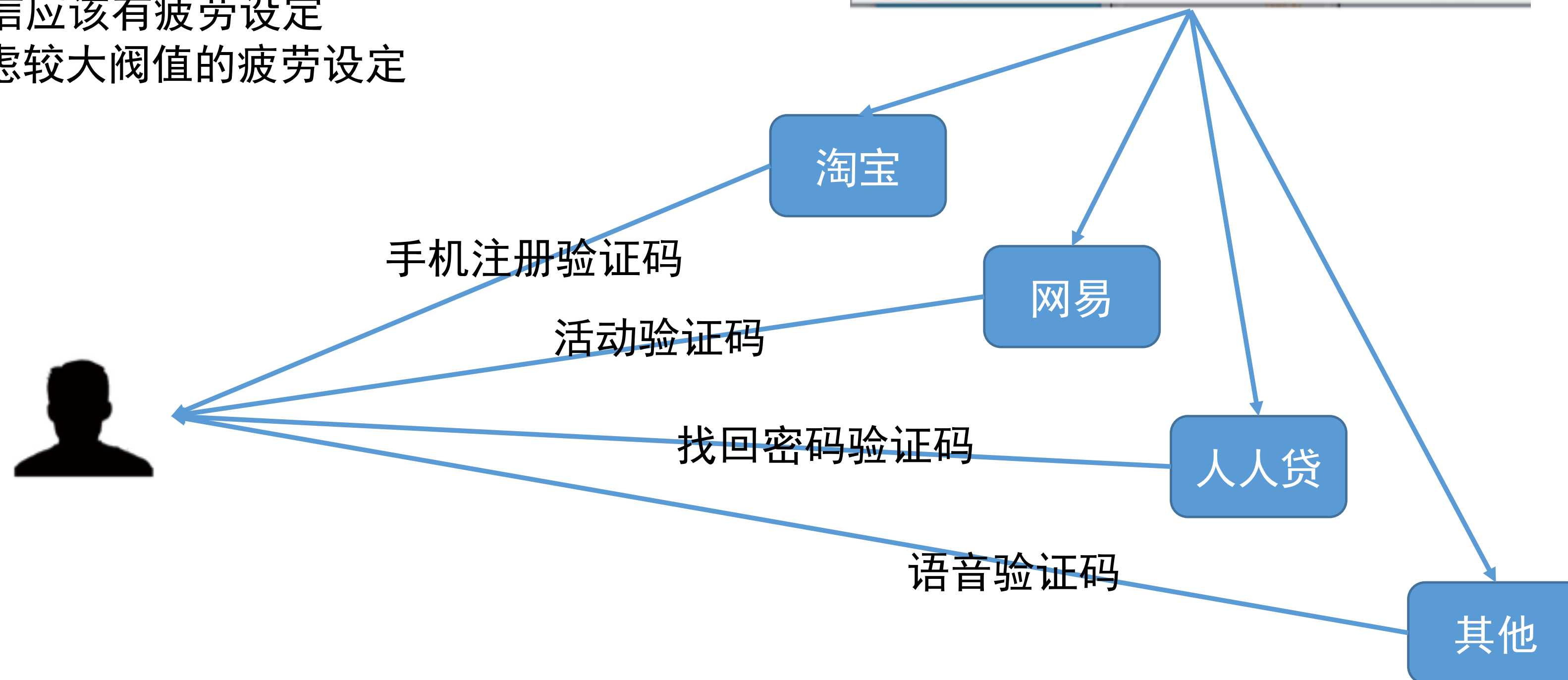
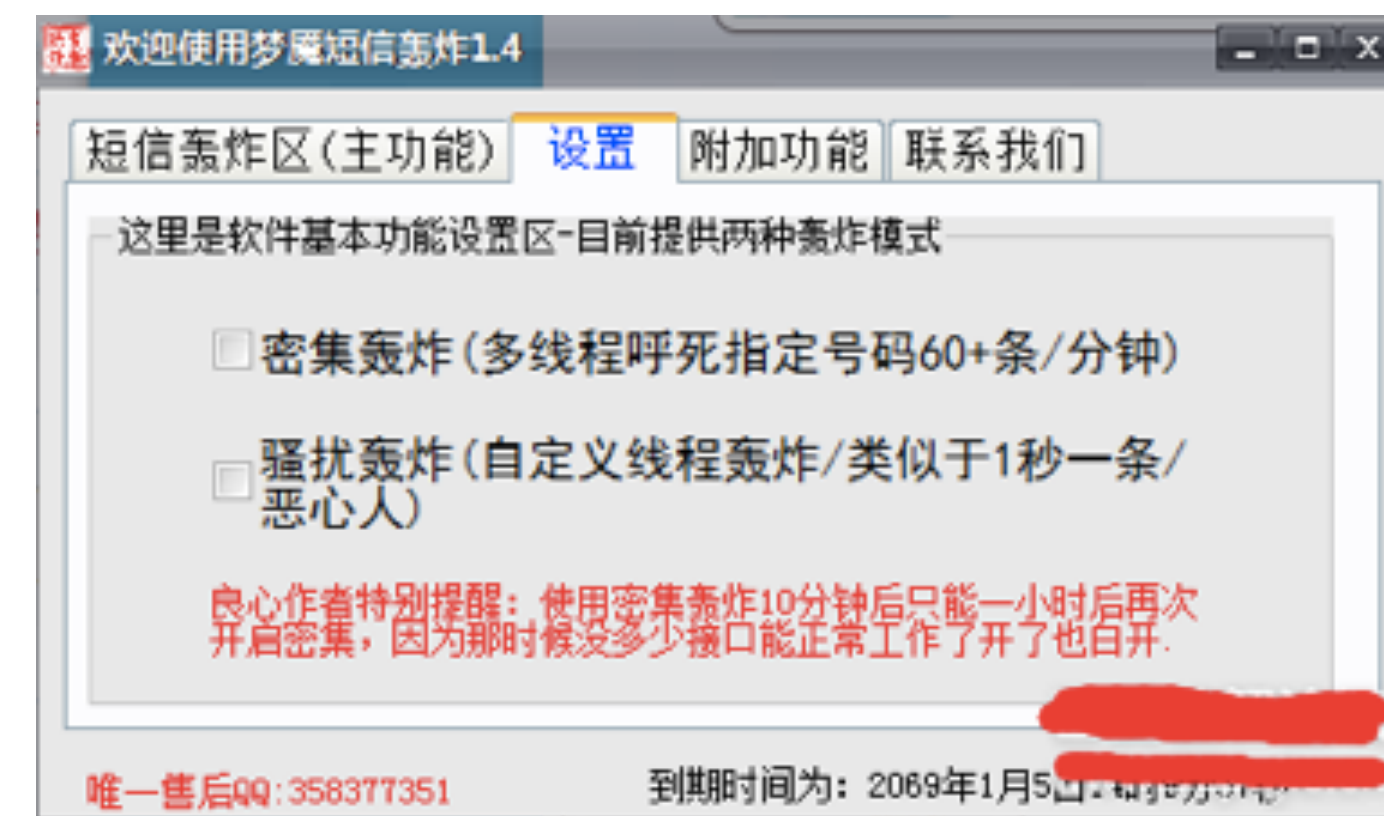
#机器人 bots



#机器人 bots

短信资费损失，正常短信发不出去
导致短信渠道异常被关闭

不仅单手机短信应该有疲劳设定
单IP也应当考虑较大阈值的疲劳设定



#处理思路

行为

来源

点击频率？
页面访问丰富程度？
是否遗漏关键访问页面？
来源IP是否有过违规事实？
是否为代理IP？
是否为机房服务器IP？

正常用户的一次页面访问

✓	方法	文件
●	POST	lsp.aspx
●	POST	lsp.aspx
● 200	GET	/?mkt=zh-CN
▲ 304	GET	hp_zh_cn.png
▲ 304	GET	hpc18.png
● 204	GET	I?IG=CE4B099CEFD4E2AA9606904577F31D3&Type=Eve...
● 204	POST	lsp.aspx
○ 200	GET	5e4f0a42.js?bu=rms+serp+Shared\$shared_c.source,Share...
○ 200	GET	b4de9387.js
○ 200	GET	5167a640.js
○ 200	GET	c76620da.js
○ 200	GET	6c680cd0.js?bu=rms+answers+BoxModel+config,rules\$rul...
○ 200	GET	b4de9387.js
○ 200	GET	5167a640.js
○ 200	GET	c76620da.js
○ 200	GET	6c680cd0.js?bu=rms+answers+BoxModel+config,rules\$rul...
● 200	GET	render?bnptrigger={"PartnerId":"HomePage","IID":"SERP.2...
● 200	GET	life?mkt=zh-CN&IID=SERP.5044&IG=CE4B099CEFD4E2A...
● 200	GET	homepagelmgViewer_c.js
○ 200	GET	88bb0675.js?bu=rms+answers+AutoSuggest+Modules\$Ser...
● 200	GET	HPImageArchive.aspx?format=js&idx=0&n=1&nc=1459149...
● 204	GET	I?IG=CE4B099CEFD4E2AA9606904577F31D3&Type=Eve...
● 200	GET	counting?p=hp&s=HomepageShare&o=r&k=s_undefined
● 200	GET	counting?p=hp&s=HomepageShare&o=r&k=undefined
● 204	POST	lsp.aspx
▲ 302	GET	Passport.aspx?popup=1
● 204	POST	lsp.aspx
● 200	GET	Passport.aspx?popup=1
▲ 302	GET	login.srf?wa=wslogin1.0&rosnv=11&ct=1459149638&ver=6...

爬虫的页面访问

/产品列表.html
/产品01详情.html
/产品02详情.html
/产品03详情.html
/产品04详情.html
/产品05详情.html
/产品06详情.html
/产品07详情.html
/产品08详情.html
...

/验证手机.html?mob=18600000001
/验证手机.html?mob=18600000002
/验证手机.html?mob=18600000003
/验证手机.html?mob=18600000004
/验证手机.html?mob=18600000005
/验证手机.html?mob=18600000006
/验证手机.html?mob=18600000007
...

/admin/
/root/
/license/
/manager/
/config.txt
/administrator/
/login/
...

#用户账户

虚假的用户身份

手机号、身份证、银行卡

2000W酒店开房信息免费查询 (重要提示: 姓名/身份证号)

姓名: 刘明 身份证号: 310101198010234567 手机号: 13816222718 验证码: 123456

姓名	性别	年龄	生日	证件	证件号	手机	地址	备注
刘明	男	38	19801023	ID	310101198010234567	13816222718	武汉市青山红钢城红钢城11号	2013-10-18 2:30:44
刘明	男	32	19801023	ID	110108198010234567	13816222718	北京市东城区东直门43号	
刘明	男	38	19801023	ID	370306198010234567	13816222718	山东省临沂市兰山区	
刘明	男	31	19801023	ID	310101198010234567	13816222718	上海市浦东新区陆家嘴	

1. 可批量生成身份证号, 并且可以指定身份证的地区和生日性别, 同时随机出一个人的名字。

城市: 上海市 市辖区: 浦东新区

生日: 1980 月: 1 日: 1

性别: ☒ 男性 ☐ 女性

生成身份证号

性别	姓名	出生日期	发证地	身份证号
男	陈春洲	1980年01月01日	上海市市辖区浦东新区	3101151980010113530
男	曹浩轩	1980年01月01日	上海市市辖区浦东新区	3101151980010110917
男	傅耀轩	1980年01月01日	上海市市辖区浦东新区	3101151980010112015

2000W开房数据

身份证在线生成器

猫池

短信收码平台

- ☐ 爱码用户管理平台项目库—爱码手机验证码短信接收平台
- ☐ 飞码手机验证码自动收发短信平台—淘宝解除异常,QQ解封解冻,陌陌验证等网上唯...
- ☒ 51验证码短信接收平台官网—代收淘宝、新浪、京东等各大网站手机验证码
- ☒ 云码手机验证码系统—会员中心
- ☒ 项目列表—飞Q手机验证码自动接收系统
- ☒ 项目列表—一查码平台
- ☒ 卓码项目列表—卓码手机验证码短信接收平台
- ☒ 项目列表—中国领先的短信验证码平台,提供短信验证码收发服务—浪码
- ☐ 猪猪美国手机验证码接收平台
- ☒ 获取验证码—手机验证码在线自动获取系统

专业代办各种银行卡

银行开借记卡 买银行卡

身份证 0元



手机号码 一条短信1元左右 批发短信卡25一张

借记卡 自办0元 黑卡300~500一张

虚假的用户身份

IP、邮箱、客户端

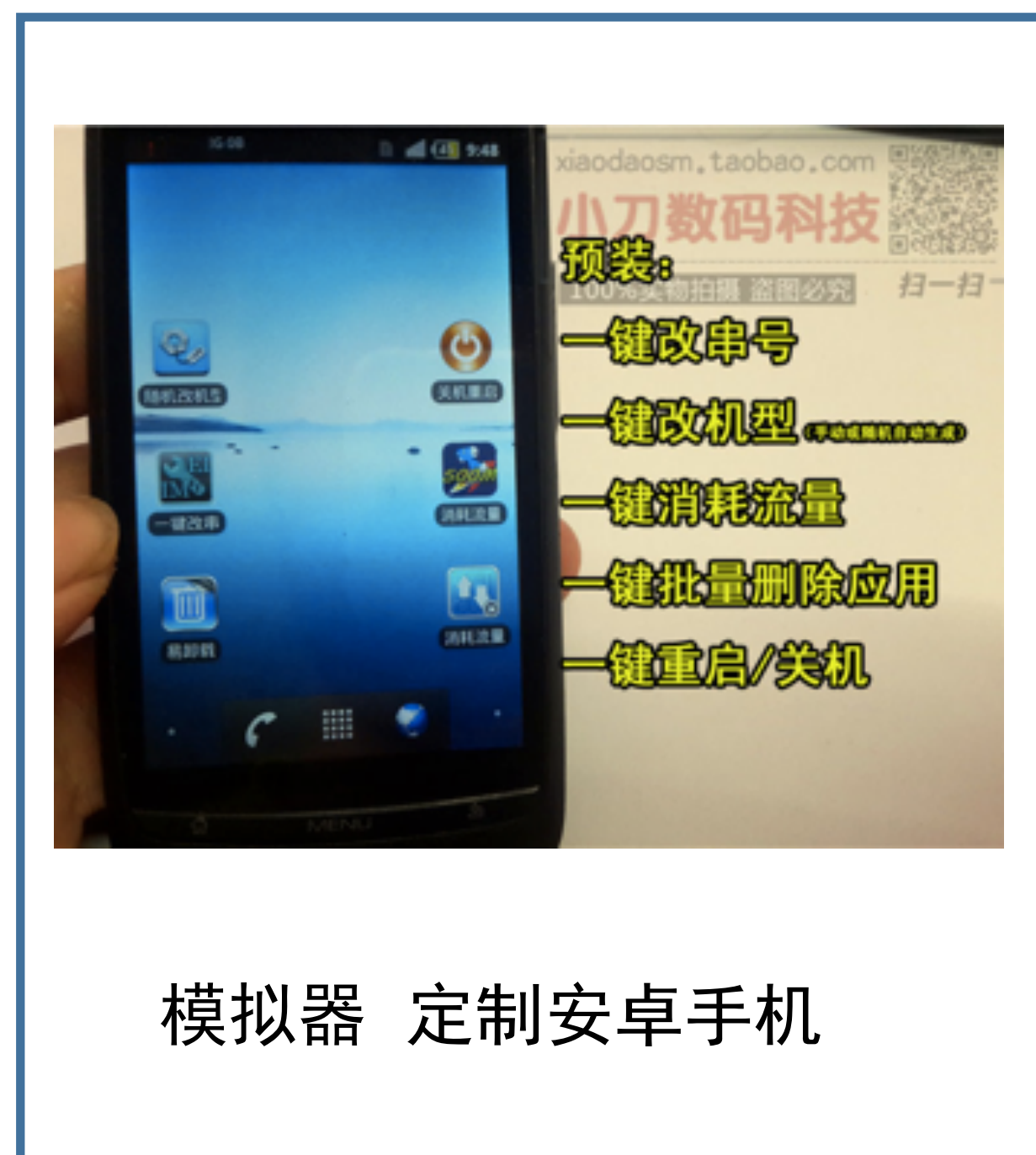


临时邮箱 / 10分钟邮箱

临时邮箱 0元



IP
20~60 块钱一个月

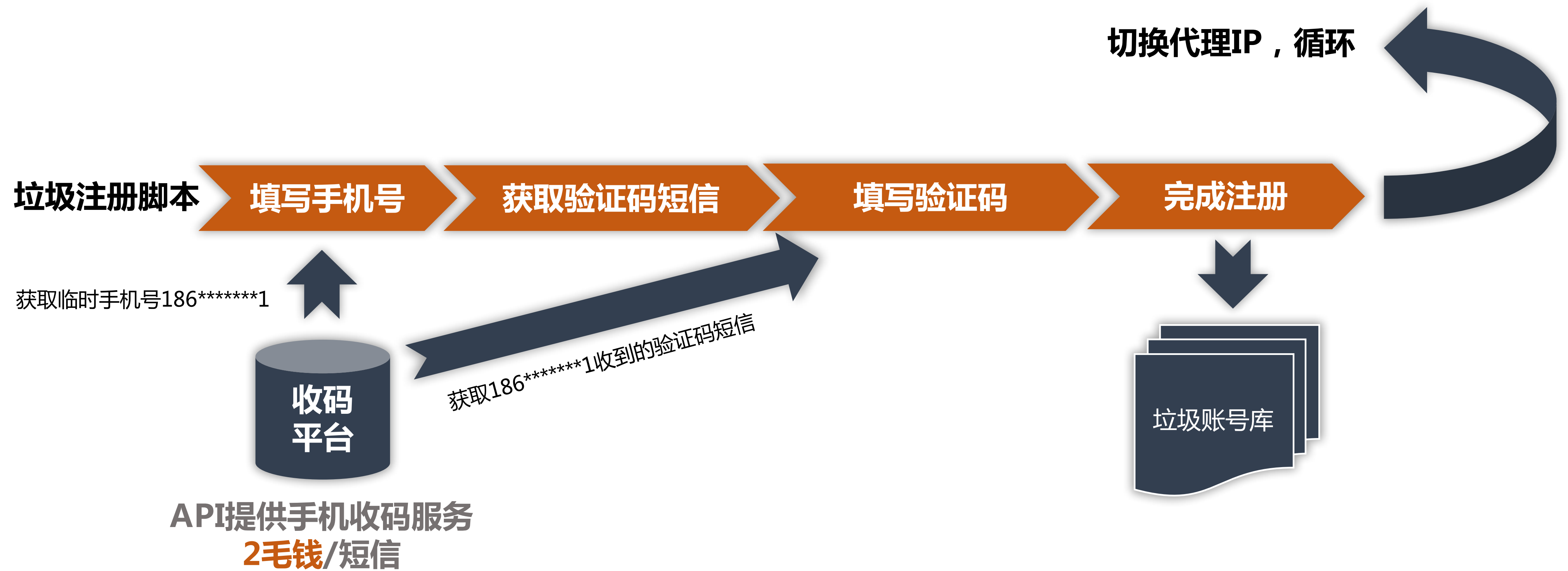


模拟器 定制安卓手机

定制安卓手机, 160元, 模拟器 0元



#虚假账户



#账户盗用



#处理思路

扫号撞库

登陆单一IP频率？
只访问登陆接口？
登陆大量不存在的账号？
用户登录与常用登陆区域不同？
超快速页面点击频率？
IP内是否有深度页面访问？

垃圾注册

同一设备关联超过5个以上账号？
某IP出现大量异地手机号码注册
相似用户名、相同密码？
无意义的用户名？

规则名称	版本号	规则说明
regist_N_static	1453886007395	单IP注册不加载静态资源
regist_S_password	1453886007395	单IP频繁注册同密码账号
regist_H_count	1453886007395	单IP短时间内频繁注册

规则名称	版本号	规则说明
visit_H_loginurl	1453886007395	单IP短时间内请求多次login类型页面
login_S_password	1458644612138	单IP尝试多次不同账号同密码登录
login_H_count	1453886007395	单IP短时间内登录次数频繁
login_N_static	1453886007395	登陆请求近期未加载静态资源，单独请求API
login_S_account	1453886007395	短时间内尝试多次登录相同账号，密码不同
login_N_referer	1453886007395	登录请求不包含referer
login_H_failure	1453886007395	单IP短时间内频繁登录失败

#羊毛党/黄牛



联系收码平台
打码平台，或者买卡
准备自动脚本

线报收集

评估准备

执行

获利

热门活动100%被光顾
其他看成本和获益比

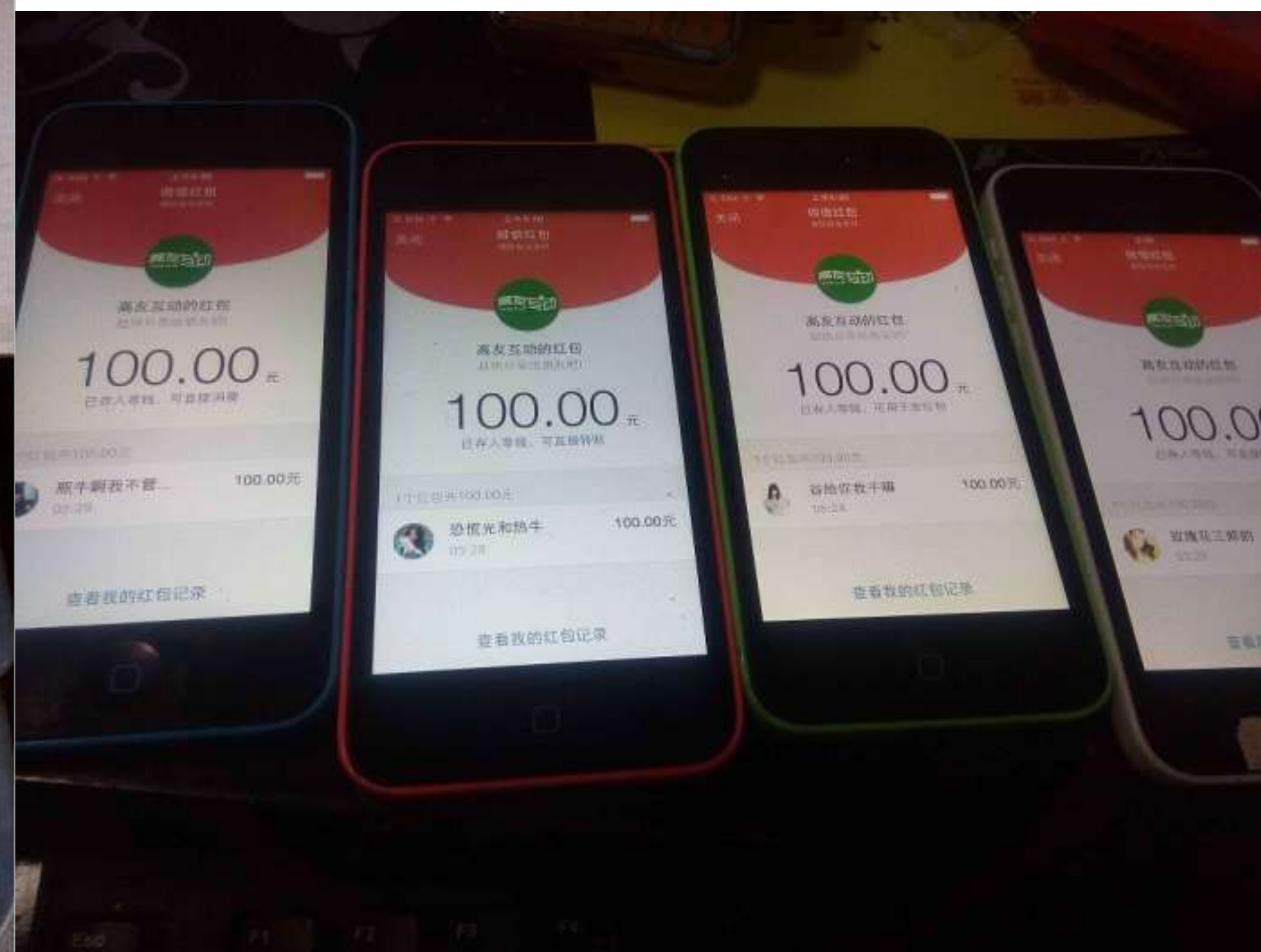
微信网赚线报获取工具 (网赚妈妈 www.wzmm.org) 群: 418980630

关键字: 现金红包/京东卡/话费 ☐更新 查询 查询 3 页 内容清空

id	双击跳转活动页面--	公众号	TIME
0	中奖万现金红包速来抢猛戳领取	沈阳车生活	2015-
1	猜灯谜抢现金红包元明星签名潮服等你来赢	中国杯帆船赛V	2015-
2	元现金红包不用摇到手抽筋晒个花灯抽大奖	江苏新闻广播	2015-
3	胖琳钱币邮票正月十五元现金红包飞起来	胖琳商贸	2015-
4	最新鲜现金红包喊出来钱你会赚多吗	浙江FM996	2015-
5	红包大战没完元宵还有万个现金红包等你抢	传递正能量	2015-
6	今晚点看电视抢万个现金红包	康宝莱营养...	2015-
7	三波好礼闹元宵送现金红包送代金券打车...	重庆机场(重...	2015-
8	喜讯爆料砸金蛋倒计时了正月十五闹元宵...	孕婴新天地	2015-
9	抽奖年后大礼第一波春春发的现金红包好...	苏昆太生活圈	2015-
10	中奖万现金红包速来抢猛戳领取	沈阳车生活	2015-
11	猜灯谜抢现金红包元明星签名潮服等你来赢	中国杯帆船赛V	2015-
12	元现金红包不用摇到手抽筋晒个花灯抽大奖	江苏新闻广播	2015-
13	胖琳钱币邮票正月十五元现金红包飞起来	胖琳商贸	2015-
14	最新鲜现金红包喊出来钱你会赚多吗	浙江FM996	2015-
15	红包大战没完元宵还有万个现金红包等你抢	传递正能量	2015-
16	今晚点看电视抢万个现金红包	康宝莱营养...	2015-
17	三波好礼闹元宵送现金红包送代金券打车...	重庆机场(重...	2015-
18	喜讯爆料砸金蛋倒计时了正月十五闹元宵...	孕婴新天地	2015-
19	抽奖年后大礼第一波春春发的现金红包好...	苏昆太生活圈	2015-
20	红包元宵抢万个现金红包最高金额元准备...	柘荣索罗	2015-
21	周嘉福现金红包今日开抢	周嘉福说琥珀	2015-
22	元宵节猜灯谜拿现金红包	武汉中央文化区	2015-
23	红包大战没完元宵还有万个现金红包等你抢	临汾吃喝玩乐	2015-
24	另一波绵壹城现金红包元宵当天线下抢	宁波最热门	2015-
25	红包大战没完小编偷偷告诉你还有万现金...	海岸咖啡语茶	2015-



小白成长篇，芬芬o(n_n)o 哈哈



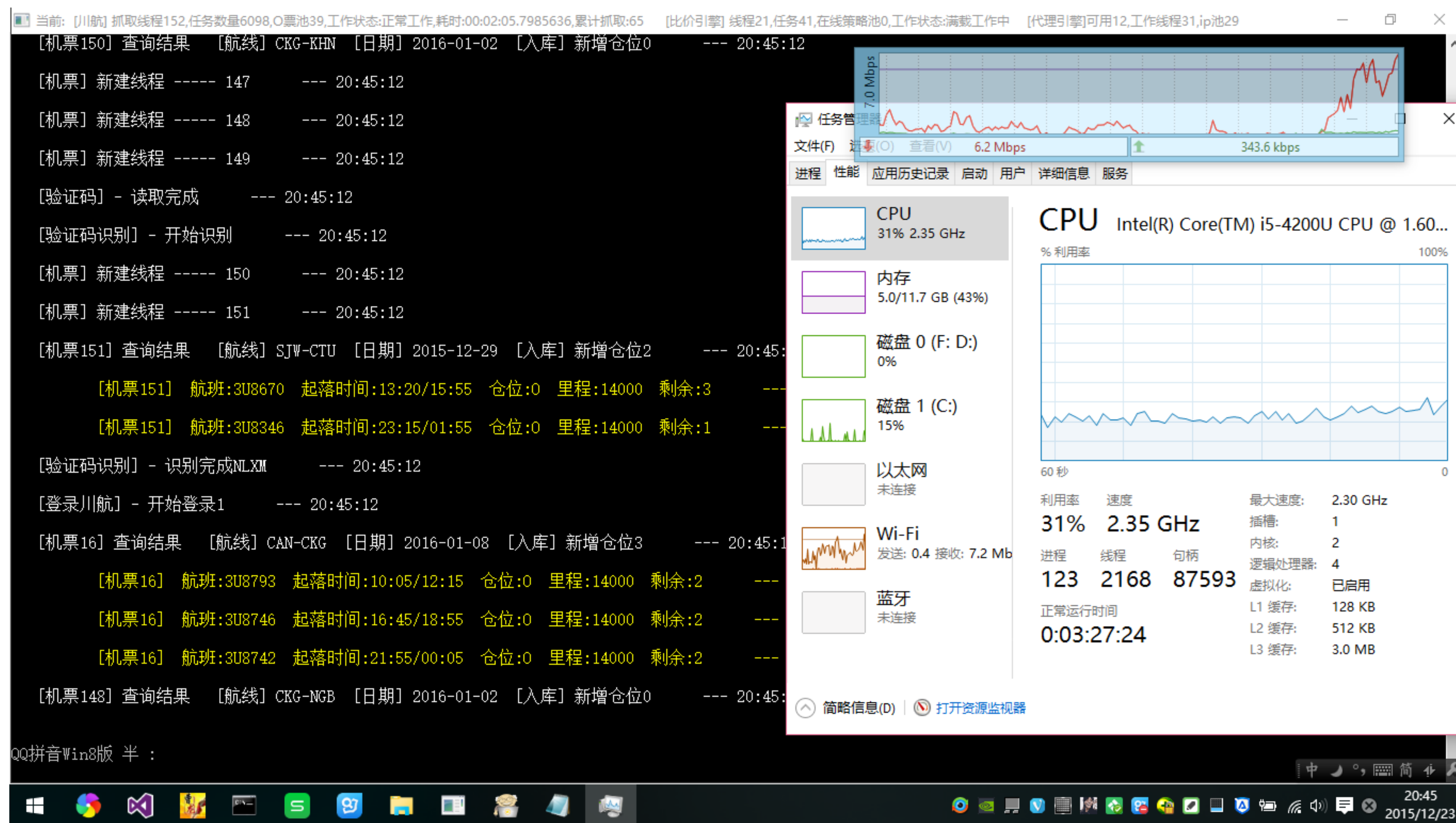
#恶意订单



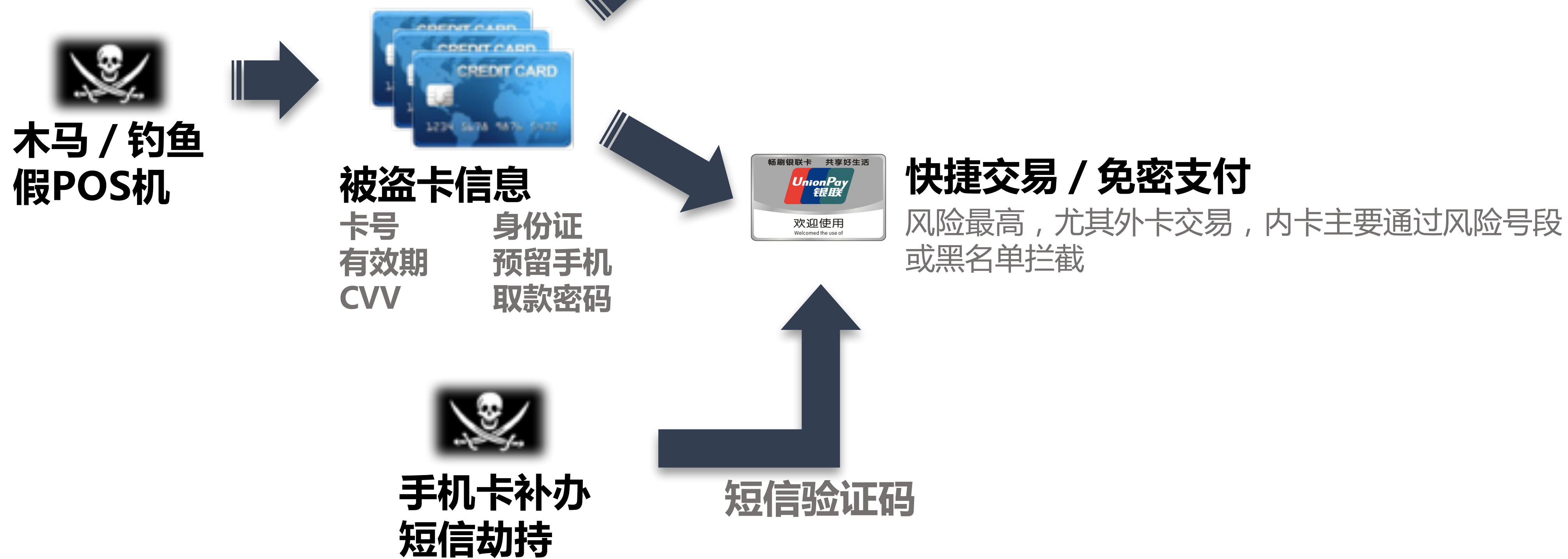
对有限库存的商品进行自动监控

自动下单

与正常用户的访问轨迹有非常大的区别



#虚假交易



每个人都有可能是坏的

了解，知道，处置

情报服务

本地分析瓶颈的有效补充



黑名单联盟

交换信任问题
不能完全定性

成本低廉

192.168.0.1
188 8888 8888

IP/手机情报

云服务器 / 机房IP
组织出口
代理服务器
收码平台手机
欺诈电话平台数据
颗粒度大，需要结合使用



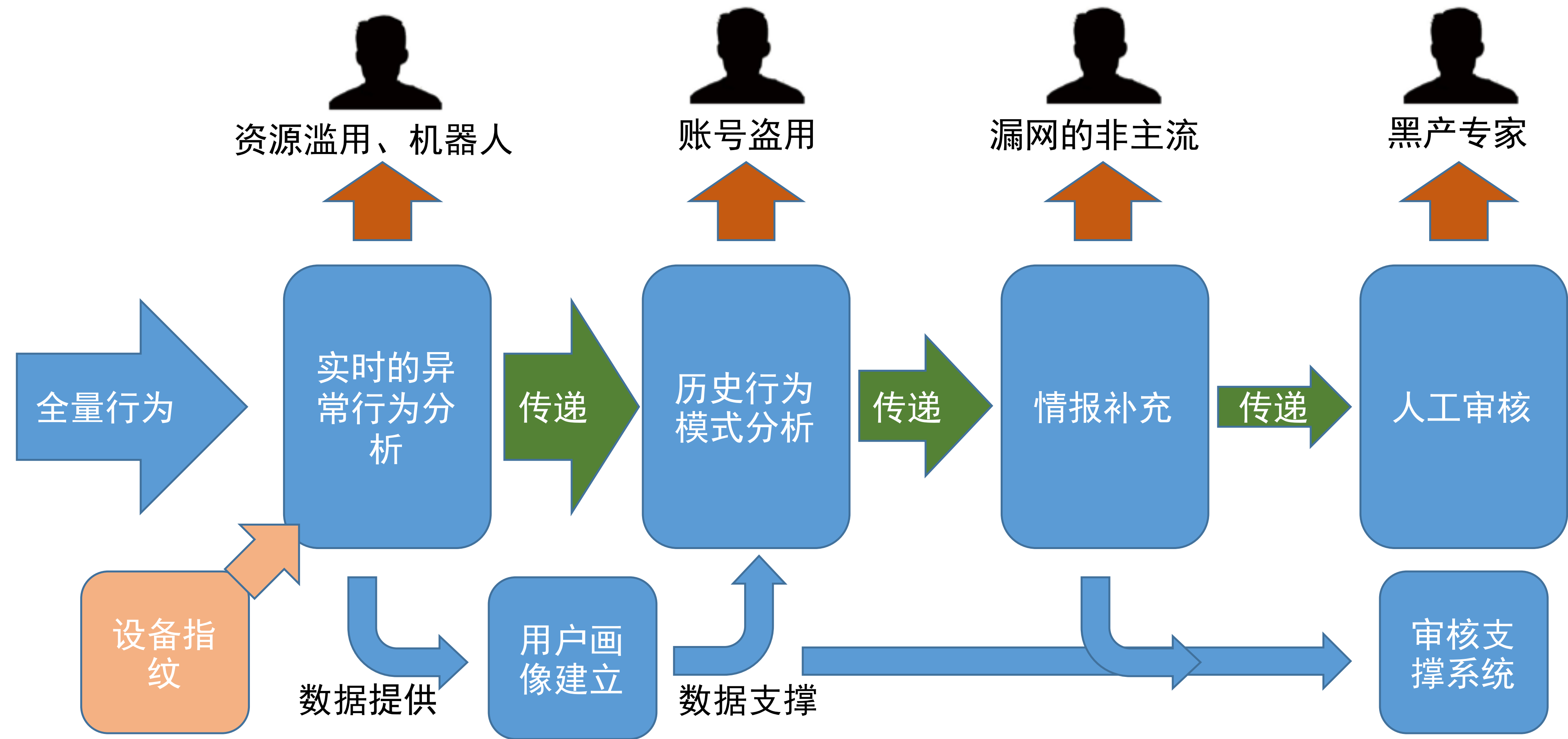
失信情报

法院传票
欠款逾期
不良记录

局限性(初犯)

构建我们工具

要种常青树，就要给予合理的投入





谢谢！

